

01/22/99

Appendix I

01/22/99
Appendix I
JCS300 U.S. PTO

Java™ Card™ Runtime Environment (JCERe)

2.1 Specification

Draft 2

Copyright © 1998 Sun Microsystems, Inc.
901 San Antonio Road, Palo Alto, CA 94303 USA

All rights reserved. Copyright in this document is owned by Sun Microsystems, Inc.

Sun Microsystems, Inc. (SUN) hereby grants to you at no charge a non-exclusive, non-transferable, limited license (without the right to sublicense) under SUN's intellectual property rights that are essential to practice the Java™ Card™ Runtime Environment (JCERe) 2.1 Specification ("Specification") to use the Specification for internal evaluation purposes only. Other than this limited license, you acquire no right, title, or interest in or to the Specification and you shall have no right to use the Specification for productive or commercial use.

RESTRICTED RIGHTS LEGEND

This document is subject to restrictions of FAR 52.227-14(g)(2)(ii)(B) and FAR 52.227-19(e)(7), or DFAR 732.227-701(b)(6)(v) and DFAR 721.7202-1(e).

SUN MAKES NO REPRESENTATIONS OR WARRANTIES ABOUT THE SURVIVALABILITY OF THE SOFTWARE, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR ANY PARTICULAR PURPOSE, OR NON-INFRINGEMENT. SUN SHALL NOT BE LIABLE FOR ANY DAMAGES SUFFERED BY LICENSEE AS A RESULT OF USING, MODIFYING OR DISTRIBUTING THIS SOFTWARE OR ITS DERIVATIVES.

TRADEMARKS

Sun, the Sun logo, Sun Microsystems, JavaSoft, JavaBeans, JDK, Java, Java Card, HotJava, HotJava View, Visual Java, Solaris, NEO, Inc., Netra, NFS, ONC, ONC+, OpenWindows, PC-NFS, Embodiddles, PersonalJava, RDBMS, Scaled Manager, Soliris,awards, SunOS, SunOne, SunCare, SunNet, SunView, SunWorkstation, The Network Is The Computer, ToolTalk, Ultra, UltraCom, UltraComWilling, UltraServer, UltraThe Network Is The Computer, UltraWorkShop, The Java Coffee Cup logo, and Visual Java are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.

THIS PUBLICATION IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT.

THIS PUBLICATION COULD INCLUDE TECHNICAL INACCURACIES OR TYPOGRAPHICAL ERRORS. CHANGES AND PERIODICALLY ADDED TO THE INFORMATION HEREIN; THESE CHANGES WILL BE INCORPORATED IN NEW EDITIONS OF THE PUBLICATION. SUN MICROSYSTEMS, INC. MAY MAKE IMPROVEMENTS AND/OR CHANGES IN THE PRODUCT(S) AND/OR THE PROGRAM(S) DESCRIBED IN THIS PUBLICATION AT ANY TIME.

Sun Microsystems, Inc.
901 San Antonio Road
Palo Alto, CA 94303 USA
650 960-1400

Draft 2, Revision 14, 1998

Java™ Card™ Runtime Environment (JCРЕ) 2.1 Specification

Contents

1. Introduction	1-1
2. Lifetime of the Java Card Virtual Machine	2-1
3. Java Card Applet Lifetime	3-1
3.1 The Method <code>install()</code>	3-1
3.2 The Method <code>select()</code>	3-2
3.3 The Method <code>process()</code>	3-2
3.4 The Method <code>deselect()</code>	3-3
3.5 Power Loss and Reset	3-3
4. Transient Objects	4-1
4.1 Events That Clear Transient Objects	4-2
5. Selection	5-1
5.1 The Default Applet	5-1
5.2 SELECT Command Processing	5-2
5.3 Non-SELECT Command Processing	5-3
6. Applet Redirection and Object Sharing	6-1
6.1 Applet Firewall	6-1
6.1.1 Currents and Context Switching	6-1
7. Transactions and Atomicity	7-1
7.1 Atomicity	7-1
7.2 Transactions	7-1
7.3 Transaction Duration	7-2
7.4 Nested Transactions	7-2
7.5 Tear or Reset Transaction Failure	7-2
7.6 Aborting a Transaction	7-3
7.6.1 Programmatic Abortion	7-3
7.6.2 Abortion by the JCРЕ	7-3
7.6.3 Cleanup Responsibilities of the JCРЕ	7-3
7.7 Transient Objects	7-3
7.8 Cache Capacity	7-3
8. API Topics	8-1
8.1 The APDU Class	8-1
8.1.1 T=0 specifies for ongoing data transfers	8-1

Java™ Card™ Runtime Environment (JCРЕ) 2.1 Specification

6.1.2 Object Ownership	6-1
6.1.3 Object Access	6-2
6.1.4 Finalization	6-2
6.1.5 Static Fields and Methods	6-3
6.2 Object Access Across Contexts	6-3
6.2.1 JCРЕ Entity Point Objects	6-4
6.2.2 Global Arrays	6-5
6.2.3 JCРЕ Privileges	6-5
6.2.4 Shareable Interfaces	6-5
6.2.5 Detaching from the Previous Context	6-5
6.2.6 Shareable Interface Details	6-7
6.2.7 Obtaining Shareable Interface Objects	6-7
6.2.8 Object Access Behavior	6-8
6.3 Transient Objects and Applet contexts	6-12
7. Transactions and Atomicity	7-1
7.1 Atomicity	7-1
7.2 Transactions	7-1
7.3 Transaction Duration	7-2
7.4 Nested Transactions	7-2
7.5 Tear or Reset Transaction Failure	7-2
7.6 Aborting a Transaction	7-3
7.6.1 Programmatic Abortion	7-3
7.6.2 Abortion by the JCРЕ	7-3
7.6.3 Cleanup Responsibilities of the JCРЕ	7-3
7.7 Transient Objects	7-3
7.8 Cache Capacity	7-3

Java™ Card™ Runtime Environment (JCRE) 2.1 Specification

8.1.2 T=1 specifies for outgoing data transfers	8-3
8.2 The security and crypto packages	8-4
8.3 JCSystem Class	8-5
9. Virtual Machine Topics	
9.1 Resource Failures	9-1
10. Applet Installed	10-1
10.1 The Installer	10-1
10.1.1 Installer Implementation	10-1
10.1.2 Installer AID	10-2
10.1.3 Installer APDU	10-2
10.1.4 Installer Behavior	10-2
10.1.5 Installer Privileges	10-3
10.2 The Newly Installed Applet	10-3
10.2.1 Initialization Parameters	10-3
11. API Contracts	

Java™ Card™ Runtime Environment (JCRTU) 2.1 Specification

Preface

Java™ Card™ technology combines a portion of the Java programming language with a runtime environment optimized for smart cards and related, small memory embedded devices. The goal of Java Card technology is to bring many of the benefits of Java software programming to the resource-constrained world of smart cards.

This document is a specification of the Java Card Runtime Environment (JCRE) 2.1. A vendor of a Java Card-enabled device provides an implementation of the JCRC. A JCRC implementation within the context of this specification refers to a "vendor" implementation of the Java Card Virtual Machine (VM), the Java Card Application Programming Interface (API), or other component, based on the Java Card technology specification. A "Reference Implementation" is an implementation produced by Sun Microsystems, Inc. APIs written for the Java Card platform are referred to as Java Card APIs.

Who Should Use This Specification?

This specification is intended to assist JCRC implementers in creating an implementation, developing a specification to extend the Java Card technology specifications, or in creating an extension to the Java Card Runtime Environment (JCRC). This specification is also intended for Java Card applet developers who want a greater understanding of the Java Card technology specifications.

Before You Read This Specification

Before reading this guide, you should be familiar with the Java programming language, the Java Card technology specification, and smart card technology. A good resource for becoming familiar with Java technology and Java Card technology is the Sun Microsystems, Inc. website, located at:

<http://java.sun.com>

How This Specification Is Organized

Chapter 1, "The Scope and Responsibilities of the JCRC," gives an overview of the services required of a JCRC implementation.

Chapter 2, "Lifetime of the Virtual Machine," defines the lifetime of the Virtual Machine.

Java™ Card™ Runtime Environment (JCRE) 2.1 Specification

Chapter 3, "Applet Lifetime," defines the lifetime of an applet.

Chapter 4, "Transient Objects," provides an overview of transient objects.

Chapter 5, "Selection," describes how the JCRE handles applet selection.

Chapter 6, "Applet Isolation and Object Sharing," describes applet isolation and object sharing.

Chapter 7, "Transactions and Atomicity," provides an overview of atomicity during transactions.

Chapter 8, "API Topics," describes API functionality required of JCRE but not completely specified in the *Java Card 2.1 API Specification*.

Chapter 9, "Virtual Machine Topics," describes virtual machine specific.

Chapter 10, "Applet Installer," provides an overview of the Applet Installer.

Chapter 11, "API Constants," provides the numeric value of constants that are not specified in the *Java Card 2.1 API Specification*.

Glossary is a list of words and their definitions to assist you in using this book.

Related Documents and Publications

References to various documents or products are made in this manual. You should have the following documents available:

- *Java Card 2.1 API Draft 7 Specification*, Sun Microsystems, Inc.
- *Java Card 2.0 Language Model and Virtual Machine Specification, October 13, 1997, Revision 1.0 Final*, Sun Microsystems, Inc.
- *Java Card Applet Developer's Guide*, Sun Microsystems, Inc.
- *The Java Language Specification* by James Gosling, Bill Joy, and Guy L. Steele, Addison-Wesley, 1996, ISBN 0-201-53491-1.
- *The Java Virtual Machine Specification (Java Series)* by Tim Lindholm and Frank Yellin, Addison-Wesley, 1996, ISBN 0-201-63453-X.
- *The Java Class Library: An Annotated Reference (Java Series)* by Patrick Chan and Rosanna Lee, Addison-Wesley, two volumes, ISBN: 0201310023 and 0201110011.
- ISO 7816 Specification Part 1-6.
- EN 46 Integrated Circuit Card Specification for Payment Systems.

1. Introduction

The Java Card Runtime Environment (JCРЕ) 2.1 contains the Java Card Virtual Machine (VM), the Java Card Application Programming Interface (API) classes (and industry-specific extensions), and support services.

This document, the JCРЕ 2.1 Specification, specifies the JCРЕ functionality required by the Java Card technology. Any implementation of Java Card technology shall provide this necessary behavior and environment.

2. Lifetime of the Java Card Virtual Machine

In a PC or workstation, the Java Virtual Machine runs as an operating system process. When the OS process is terminated, the Java applications and their objects are automatically destroyed.

In Java Card technology the execution lifetime of the Virtual Machine (VM) is the lifetime of the card. Most of the information stored on a card shall be preserved even when power is removed from the card. Persistent memory technology (such as EEPROM) enables a smart card to store information when power is removed. Since the VM and the objects it creates on the card are used to represent application information that is persistent, the Java Card VM appears to run forever. When power is removed, the VM stops only temporarily. When the card is next read, the VM starts up again and recovers its previous object heap from persistent storage.

Aside from its persistent nature, the Java Card Virtual Machine is just like the Java Virtual Machine.

The card initialization time is the time after making, and prior to the time of card personalization and issuance. At the time of card initialization, the JCJB is initialized. The framework objects created by the JCJB exist for the lifetime of the Virtual Machine. Because the execution lifetime of the Virtual Machine and the JCJB framework span CAD sessions of the card, the lifetimes of objects created by applets will also span CAD sessions. (CAD means Card Application Device, or card reader. Card sessions are those periods when the card is inserted in the CAD, powered up, and exchanging streams of AID's with the CAD.) Objects that have this property are called persistent objects.

The JCRC implementer shall write an object persistent when:

- The Applet.register method is called. The JCRC stores a reference to the instance of the applet object. The JCRC implementer shall ensure that instances of class support are persistent.
- A reference to an object is stored in a field of any other persistent object or in a class's static field. This requirement stems from the need to preserve the integrity of the JCRC's internal data structures.

3. Java Card Applet Lifetime

For the purposes of this specification, a Java Card applet's lifetime begins at the point that it has been correctly loaded into card memory, linked, and otherwise prepared for execution. (For the remainder of this specification, "applet" refers to an applet written for the Java Card platform.) Applets are secured with the Applet's `registerInstall` call for the lifetime of the card. The JCRE interacts with the applet via the applet's public methods `install`, `select`, `deselect`, and `process`. An applet shall implement the static `install` method. If the `install`, `select`, `deselect`, and `process` methods are not implemented, the applet's object cannot be created or initialized. A JCRE implementation shall call an applet's `install`, `select`, `deselect`, and `process` methods as described below.

When the applet is installed on the smart card, the static `install` method is called once by the JCRE for each applet instance created. The JCRE shall not call any applet's constructor directly.

3.1 The Method `install`

When `install` is called, no objects of the applet exist. The initial task of the `install` method within the applet is to create an instance of the `Applet` class, and to register the instance. All other objects that the applet will need during its lifetime can be created as is feasible. Any other preparations necessary for the applet to be selected and executed by a CAD also can be done as is feasible. The `install` method obtains initialization parameters from the contents of the incoming byte array parameter.

Typically, an applet creates various objects, initializes them with predefined values, sets some internal state variables, and calls the `Applet.register` method to specify the AID (applet identifier as defined in ISO 7816-3) to be used to select it. This installation is considered successful when the call to the `Applet.register` method completes without an exception. The installation is deemed unsuccessful if the `install` method does not call the `Applet.register` method, or if an exception is thrown from within the `install` method prior to the `Applet.register` method being called, or if the `Applet.register` method is thrown an exception. That is, all postinstall objects shall be returned to the state they had prior to calling the `install` method. If the installation is unsuccessful, the JCRE shall perform an cleanup when it regains control. That is, all postinstall objects shall be returned to the state they had prior to calling the `install` method. If the installation is unsuccessful, the JCRE can mark the applet as available for selection.

3.2 The Method `select`

Applets remain in a suspended state until they are explicitly selected. Selection occurs when the JCRE receives a `SELECT APDU` in which the name data matches the AID of the applet. Selection causes an applet to become the currently selected applet.

Prior to calling `SELECT`, the JCRE shall deselect the previously selected applet. The JCRE indicates this to the applet by invoking the applet's `deselect` method.

The JCRE informs the applet of selection by invoking its `select` method.

The applet may decline to be selected by returning `false` from the call to its `select` method or by throwing an exception. If the applet returns `true`, the actual `SELECT APDU` command is suppressed to the applet in the subsequent call to its `process` method, so that the applet can examine the APDU contents. The applet can process the `SELECT APDU` command exactly like a processor of any other APDU command. It can respond to the `SELECT APDU` with data (see the `process` method for details), or it can flag errors by throwing an `unchecked` exception with the applet-specific SW (returned status word). This SW and optional response data are returned to the CAD.

The `Applet.select` method of the `Applet` class shall return `true` when called during the `select` method. The `Applet.select` method will continue to return `true` during the subsequent `process` method, which is called to process the `SELECT APDU` command.

If the applet declines to be selected, the JCRE will return an APDU response status word of `0x00.A0.PLEASE_SELECT_PASSED` to the CAD. Upon selection failure, the JCRE must set `err` to indicate that no applet is selected.

After successful selection, all subsequent APDUs are delivered to the currently selected applet via the `process` method.

3.3 The Method `process`

All APDUs are received by the JCRE, which passes an instance of the APDU class to the `process` method of the currently selected applet.

Note - A `SELECT APDU` might cause a change in the currently selected applet prior to the call to the `process` method.

On normal return, the JCRE automatically appends the ISO9660 as the completion response SW to any data already sent by the applet.

At any time during `process`, the applet may throw an ISO9660 exception with an appropriate SW, in which case the JCRE catches the exception and returns the SW to the CAD.

If any other exception is thrown during `process`, the JCRE catches the exception and returns the status word `0x00.F0.SN_UNEXPECTED` to the CAD.

3.4 The Method deselect

When the JCRE receives a SELECT APDU command in which the name matches the AID of an applet, the JCRE calls the DESSELECT method of the currently selected applet. This allows the applet to perform any cleanup operations that may be required in order to allow some other applet to execute.

The Applet.**deselect** method shall return `false` when called during the `deselect` method. Exceptions thrown by the `deselect` method are caught by the JCRE, but the applet is deselected.

3.5 Power Loss and Reset

Power loss occurs when the card is withdrawn from the CAD or if there is some other mechanical or electrical failure. When power is re-applied to the card and on CardReset (written or read) the JCRE shall ensure that:

- Transient data is reset to the default value.
- The transaction in progress, if any, when power was lost (or reset occurred) is aborted.
- The applet that was selected when power was lost (or reset occurred) becomes implicitly deselected. (In this case the `deselect` method is not called.)
- If the JCRE implements default applet selection (see paragraph 3.1) the default applet is selected as the currently selected applet, and that the `defaultApplet.select` method is called. Otherwise, the JCRE sets its state to indicate that no applet is selected.

4. Transient Objects

4.1 Events That Clear Transient Objects

Transient objects are used for maintaining states that shall be preserved across card reads. When a transient object is created, one of two events are specified that cause its fields to be cleared: CLEAR_ON_RESET or CLEAR_ON_SELECT. These objects are used for maintaining states that shall be preserved across apply operations, but not across card reads. CLEAR_ON_DESELECT transient objects are used for maintaining states that must be preserved while an apply is selected, but not across apply selections or card reads.

Details of the two clear events are as follows:

- CLEAR_ON_RESET**—the object's fields are cleared when the card is reset. When a card is powered on, this also causes a card read.

Note—It is not necessary to clear the fields of a transient object before power is removed from a card. However, it is necessary to guarantee that the previous contents of such fields cannot be recovered once power is lost.

- CLEAR_ON_DESELECT**—the object's fields are cleared whenever any apply is deselected. Because a card read implicitly deselects the currently selected apply, the fields of CLEAR_ON_DESELECT objects are also cleared by this same event specified for CLEAR_ON_RESET.

The currently selected apply is explicitly deselected (its deselect method is called) only when a SELECT command is processed. The currently selected apply is deselected and then the fields of all CLEAR_ON_DESELECT transient objects are cleared regardless of whether the SELECT command:

- Fails to select an apply.
- Selects a different apply.
- Re-selects the same apply.

Writes to the fields of a transient object shall not have a performance penalty. (Using current smart card technology as an example, the contents of transient objects can be stored in RAM, while the contents of non-transient objects can be stored in EEPROM. Typically, RAM technology has a much faster write cycle time than EEPROM.)

Writes to the fields of a transient object shall not be affected by "Transactions." That is, an abort transaction will never cause a field in a transient object to be restored to a previous value. This behavior makes transient objects ideal for small amounts of temporary applet data that is frequently modified, but that need not be preserved across CAD or select sessions.

5.2 SELECT Command Processing

The SELECT APDU command is used to select an applet. Its behavior is:

1. The SELECT APDU is always processed by the JCRE (regardless of which, if any, applet is active).
2. The JCRE matches its internal table for a matching AID. The JCRE shall support selecting an applet where the full AID is present in the SELECT command.

JCRE implementations are free to enhance their JCRE to support other selection criterion. An example of this is selection via partial AID match as specified in ISO 7816-4. The specific requirements are as follows:

Note - An octet is indicated binary bit numbering as in ISO 7816. Most significant bit = 0b. Least significant bit = 0b1.

- a) Applet SELECT command uses CLA=0x00, INS=0x44.
- b) Applet SELECT command uses "Selection by DF name". Therefore, PI=0x04.
- c) Any other value of PI implies that it is not an applet select. The APDU is processed by the currently selected applet.
- d) JCRA shall support exact DF name (AID) selection i.e P2=0x0000 and 0x00, (0x1,0x0) are don't care.
- e) All other partial DF name SELECT options (0x1,0) are JCRA implementation dependent.
- f) All file control information option codes (P0,P1) shall be supported by the JCRA and interpreted and presented by the applet.

3. If no AID match is found:
 - a. If there is no currently selected applet, the JCRA responds to the SELECT command with status code 0x6999 (SW_APPLET_SELECT_FAILED).
 - b. Otherwise, the SELECT command is forwarded to the currently selected applet's process method.
4. Otherwise, a context switch into the applet's context occurs at this point. (The applet context is defined in paragraph 6.1.1.) Applets may use the SELECT APDU command for their own internal SELECT processing.
5. If a matching AID is found, the JCRE prepares to select the new applet. If there is an currently selected applet, it is deselected via a call to its deselect method. A context switch into the deselected applet's context occurs at this point. The JCRE context is restored upon exit from deselect.
6. The JCRE sets the new currently selected applet. This new applet is activated via a call to its select method, and a context switch into the new applet's context occurs.
 - a. If the applet's select method throws an exception or returns false, then JCRE state is set so that no applet is selected. The JCRE responds to the SELECT command with status code 0x6999 (SW_APPLET_SELECT_FAILED).
 - b. The new currently selected applet's process method is then called with the SELECT APDU as an input parameter. A context switch into the applet's context occur.

Notes -

Java™ Card™ Runtime Environment (JCRE) 2.1 Specification

If there is no matching AID, the SELECT command is forwarded to the currently selected applet (if any) for processing as a normal applet APDU command.

If there is a matching AID and the SELECT command fails, the JCRAF always enters the state where no applet is selected.

If the matching AID is the same as the currently selected applet, the JCRAF will goes through the process of de-selecting the applet and then selecting it. Reselection could fail, leaving the card in a state where no applet is selected.

5.3 Non-SELECT Command Processing

When a non-SELECT APDU is received and there is no currently selected applet, the JCRAF shall respond to the APDU with status code 0x0999 (SW_APPLET_SELECT_FAILED).

When a non-SELECT APDU is received and there is a currently selected applet, the JCRAF invokes the process method of the currently selected applet passing the APDU as a parameter. This causes a context switch from the JCRAF context to the currently selected applet's context. When the process method exits, the VM switches back to the JCRAF context. The JCRAF sends a response APDU and waits for the next command APDU.

Most method invocations in Java Card technology do not cause a context switch. Context switches only occur during invocation of and return from certain methods, as well as during exception calls from those methods (see 6.2.8).

During a context-switching method invocation, an additional piece of data, indicating the currently active content, is pushed onto the return stack. This context is restored when the method is exited. Further details of contexts and context switching are provided in later sections of this chapter.

6. Applet Isolation and Object Sharing

Any implementation of the JCRE shall support isolation of content and applets. Isolation means that one applet can not access the fields or objects of another applet in another content unless the other applet explicitly provides an interface for notes. The JCRE mechanisms for applet isolation and object sharing are detailed in the sections below.

6.1 Applet Firewall

The *applet firewall* within Java Card technology is runtime-enforced protection used to separate from the Java technology protection. The Java language protection still applies to Java Card applets. The Java language ensures that strong signing and protection attributes are enforced.

Applet firewalls are always enforced in the Java Card VM. They allow the VM to automatically perform additional security checks at runtime.

6.1.1 Contexts and Context Switching

Firewalls essentially partition the Java Card platform's object space into separate protected object spaces called contexts. The firewall is the boundary between one content and another. The JCRE shall allocate and manage an applet owner for each applet that is installed on the card. (But see paragraph 6.1.2 below for a discussion of group contexts.)

In addition, the JCRE maintains its own JCRE context. This context is much like an applet content, but it has special system privileges to do what it can perform operations that are denied to applet contexts.

At any point in time, there is only one active context within the VM. (This is called the *currently active content*.) All bytecode that access objects are checked by runtime against the currently active content in order to determine if the access is allowed. A `java.lang.SecurityException` is thrown when an access is disallowed.

When certain well-defined conditions are met during the execution of invoke-type bytecodes as described in paragraph 6.2.8, the VM performs a content switch. The previous content is pushed onto an internal VM stack, a new content becomes the currently active content, and the invoked method executes in this new content. Upon exit from that method the VM performs a returning content switch. The original content (or the owner of the method) is popped from the stack and is restored as the currently active content. Content switches can be nested. The maximum depth depends on the amount of VM stack space available.

6.1.2 Object Ownership

When a new object is created, it is associated with the currently active content. But the object is owned by an applet instance within the currently active content when the object is instantiated. An object is owned by an applet instance, or by the JCRE.

6.1.3 Object Access

In general, an object can only be accessed by its owning content, that is, when the owning content is the currently active content. The firewall prevents an object from being accessed by another applet in a different content.

In implementation terms, each time an object is accessed, the object's owner content is compared to the currently active content. If these do not match, the access is not performed and a `SecurityException` is thrown.

An object is accessed when one of the following bytecodes is executed using the object's reference:

- `getfield`, `putfield`, `invokevirtual`, `invokespecial`,
- `arraylength`, `checkcast`, `instanceof`
- `new` refers to the various types of array bytecodes, such as `baarray`, `caarray`, etc.

This list includes any special or optimized forms of these bytecodes implemented in the Java Card VM, such as `getfield_a`, `putfield_a`, etc.

6.1.4 Firewall Protection

The Java Card firewall provides protection against the most frequently anticipated security concern: developer mistakes and design oversights that might allow sensitive data to be "leaked" to another applet. An applet may be able to obtain an object reference from a publicly accessible location, but if the object is owned by a different applet, the firewall assures security.

Java™ Card™ Runtime Environment (JCRE) 2.1 Specification

Java™ Card™ Runtime Environment (JCRE) 2.1 Specification

The firewall also provides protection against incorrect code. If incorrect code is loaded onto a card, the firewall still protects objects from being accessed by this code.

The Java Card API 2.1 specifies the basic minimum protection requirements of contexts and firewalls because these features shall be supported in ways that are not transparent to the supplier developer. Developers shall be aware of the behavior of objects, APIs, and exceptions related to the firewall.

KCRE implementers are free to implement additional security mechanisms beyond those of the supplier firewall, as long as these mechanisms are transparent to applets and do not change the externally visible operation of the VM.

6.1.5 Static Fields and Methods

It should also be noted that classes are not owned by contexts. There is no runtime context check that can be performed when a class static field is accessed. Neither is there a context switch when a static method is invoked. (Similarly, a context switch causes no context switch.)

Public static fields and public static methods are accessible from any context: static methods execute in the same context as their caller.

Objects referenced in static fields are just regular objects. They are owned by whatever created them and standard firewall access rules apply. If it is necessary to share them across multiple applet contexts, then these objects need to be *Shareable Interface Objects* (SIO). (See paragraph 6.2.4 below.)

Of course, the conventional Java technology guarantees are still enforced for static fields and methods. In addition, when applets are isolated, the Isolator utilizes that each attempt to link to an external static field or method is permitted. Isolation and specifics about linkage are beyond the scope of this specification.

6.1.5.1 Optional static access checks

The JCRE may perform optional runtime checks that are redundant with the constraints enforced by a verifier. A Java Card VM may detect when code violates fundamental language restriction, such as invoking a private method in another class, and report an otherwise admissible violation.

6.2 Object Access Across Contexts

To enable applets to interact with each other and with the JCRE, some well-defined yet secure mechanisms are provided so one context can access an object belonging to another context.

These mechanisms are provided in the Java Card API 2.1 and are discussed in the following sections:

- JCRE Entry Point Objects
- Global Arrays
- KCRE Privileges
- Shareable Interfaces

JCRE Entry Point Objects

Secure computer systems shall have a way for user-privileged user processes (that are restricted to a subset of resources) to request system services performed by privileged "system" entities.

In the Java Card API 2.1, this is accomplished using *JCRE Entry Point Objects*. These are objects owned by the JCRE context, but they have been flagged as containing entry point methods.

The firewall protects these objects from access by applets. The entry point designation allows the methods of these objects to be invoked from any context. When that occurs, a context switch to the JCRE context is performed. These methods are the gateways through which applets request privilege JCRE system services.

There are two categories of JCRE Entry Point Objects:

Temporary JCRE Entry Point Objects

Like all JCRE Entry Point Objects, methods of temporary JCRE Entry Point Objects can be invoked from any applet context. However, references to these objects cannot be stored in class variables, instance variables, or array components. The JCRE detects and catches attempts to store references to these objects as part of the firewall functionality to prevent unauthorized re-use.

The APDU object and all JCRE-owned exception objects are examples of temporary JCRE Entry Point Objects.

Permanent JCRE Entry Point Objects

Like all JCRE Entry Point Objects, methods of permanent JCRE Entry Point Objects can be invoked from any applet context. Additionally, references to these objects can be stored and freely re-used. Permanent JCRE Entry Point Objects are examples of permanent JCRE Entry Point Objects.

The JCRE is responsible for:

- Determining what privileged services are provided to applets.
- Defining classes containing the entry point methods for those services.
- Creating one or more object instances of these classes.
- Designating these instances as JCRE Entry Point Objects.
- Designating JCRE Entry Point Objects as temporary or permanent.
- Making references to those objects available to applets as needed.

Note — Only the methods of these objects are accessible through the firewall. The fields of these objects are still affected by the firewall and can only be accessed by the JCRE context.

Only the JCRE itself can designate Entry Point Objects and whether they are temporary or permanent. JCRE implementers are responsible for implementing the mechanism by which JCRE Entry Point Objects are designated and how they become temporary or permanent.

6.2.2 Global Arrays

The global nature of some objects requires that they be accessible from any applet context. The firewall would ordinarily prevent these objects from being used in a flexible manner. The Java Card VM allows an object to be designated as *global*.

All global arrays are temporary global array objects. These objects are owned by the JCRE context, but can be accessed from any applet context. However, references to these objects cannot be stored in class variables.

Java™ Card™ Runtime Environment (JCRE) 2.1 Specification

Java™ Card™ Runtime Environment (JCRE) 2.1 Specification

instance variables or array components. The XMLE detector and restricts attempts to store references to the objects as part of the firewall functionality to prevent unauthorized re-use.

For added security, only arrays can be designated as global and only the JCRE itself can designate global arrays. Because applets cannot create them, no API methods are defined. JCRE implementers are responsible for implementing the mechanism by which global arrays are designated.

At the time of publication of this specification, the only global arrays required in the Java Card API 2.1 are the AID buffer and the byte array input parameter (bxr or rsv) to the applet's install method.

Note—Because of its global status, the API specifies that the APDU buffer is cleared to zero whenever an applet is selected, before the JCRE accepts a new APDU command. This is to prevent an applet's potentially sensitive data from being "leaked" to another applet via the global APDU buffer. The APDU buffer can be accessed from a shared interface object context and is available for passing data across applet contexts. The applet is responsible for protecting secret data that may be accessed from the APDU buffer.

6.2.3 JCRE Privileges

Because it is the "owner" context, the JCRE context has a special privilege. It can invoke a method of any object on the card. For example, assume that object X is owned by applet A. Normally, only owner A can invoke the fields and methods of X. But the JCRE context is allowed to invoke any of the methods of X. During an invocation, a context switch occurs from the JCRE context to the applet context that owns X.

Note—The JCRE can access both *methods* and *fields* of X. Method access is the mechanism by which the JCRE enters an applet context. Although the JCRE could invoke any method through the firewall, it shall only invoke the *select*, *process*, *deactivate*, and *getShareableInterfaceObject* (see 6.2.7.1) methods defined in the Applet class.

The JCRE context is the currently active context when the VM begins running after a *readCard*. The JCRE context is the "top" context and is always either the currently active context or the bottom context saved on the stack.

6.2.4 Shareable Interfaces

Shareable interfaces are a new feature in the Java Card API 2.1 to enable applet interaction. A shareable interface defines a set of shared interface methods. These interface methods can be invoked from one applet context even if the object implementing them is owned by another applet context.

In this specification, an object instance of a class implementing a shareable interface is called a *Shareable Interface Object* (SIO).

To the owning context, the SIO is a normal object whose fields and methods can be accessed. To any other context, the SIO is an instance of the shareable interface, and only the methods defined in the shareable interface are accessible. All other fields and methods of the SIO are protected by the firewall.

Shareable interfaces provide a secure mechanism for inter-applet communication, as follows:

1. To make an object available to another applet, applet A first defines a shareable interface, SI. A shareable interface extends the interface JavaCard, IShareable. The methods defined in the shareable interface, SI, represent the services that applet A makes available to other applets.
2. Applet A then defines a class C that implements the shareable interface SI. Class C implements the methods defined in SI. C may also define other methods and fields, but these are protected by the applet firewall. Only the methods defined in SI are accessible to other applets.

6.2.5 Determining the Previous Context

When an applet calls *getSystem.getPreviousContext* or *AID*, the JCRE shall return the instance AID of the applet instance active at the time of the last context switch.

The JCRE context does not have an AID. If an applet calls the *getPreviousContext* or *AID* method when the applet context was entered directly from the JCRE context, this method returns null.

If the applet calls *getPreviousContext* or *AID* from a method that may be accessed either from within the applet itself or when accessed in a shareable interface from an external applet, it shall check for null return before performing caller AID authentication.

6.2.6 Shareable Interface Details

6.2.6.1 The Java Card Shareable Interface

The shareable interface is simply one that extends (either directly or indirectly) the `TaggedInterface`. A shareable interface serves to identify all shared objects. Any object that needs to be shared through the applet firewall shall directly or indirectly implement this interface. Only those methods specified in a shareable interface are available through the firewall.

Implementation classes can implement any number of shareable interfaces and can extend other shareable implementation classes.

Like any Java platform interface, a shareable interface simply defines a set of service methods. A service provider class derives that it "implements" the shareable interface and provides implementations for each of the service methods of the interface. A service client class accesses the service by obtaining an object reference, casting it to the shareable interface type if necessary, and invoking the service methods of the interface.

The shareable interfaces within the Java Card technology shall have the following properties:

- When `c1` is invoked in a shareable interface is invoked, a context switch occurs to the context of the object's owner.
- When the method exits, the context of the caller is restored.
- Exception handling is enhanced so that the currently active context is correctly restored during the stack frame unwinding that occurs as an exception is thrown.

6.2.7 Obtaining Shareable Interface Objects

Inter-applet communication is accomplished when a client applet invokes a shareable interface method of a SIO belonging to a server applet. In order for this to work, there must be a way for the client applet to obtain the SIO from the server applet in the first place. The JCER provides a mechanism to make this possible. The `Applet` class and the `AppletContext` class provide methods to enable a client to request services from the server.

6.2.7.1 The Method `Applet.getShareableInterfaceObject`

This method is implemented by the server applet instance. It shall be called by the JCER to mediate between a client applet that requests to use an object belonging to another applet, and the server applet that makes its objects available for sharing.

The default behavior shall return null, which indicates that an applet does not participate in inter-applet communication.

A server applet that is intended to be invoked from another applet needs to override this method. This method should examine the `c1` and `c2` parameters. If the client `c1` is not one of the expected AIDs, the method should return null. Similarly, if the parameter `c2` is not recognized or if it is not allowed for the

`c1` and `c2`, then the method also should return null. Otherwise, the applet should return an SIO of the shareable interface type that the client has requested.

The server applet need not respond with the same SIO to all clients. The server can support multiple types of shareable interfaces for different purposes and use `c1` and `c2` parameter to determine which kind of SIO to return to the client.

6.2.7.2 The Method `JCSysEnv.getAppletShareableInterfaceObject`

The `JCSysEnv` class contains the method `getAppletShareableInterfaceObject`, which is invoked by a client applet to communicate with a server applet.

The JCER shall implement this method to behave as follows:

1. The JCER searches its internal applet table for one with `serverAID`. If not found, null is returned.
2. The JCER invokes this applet's `getShareableInterfaceObject` method, passing the `c1` back to its caller and the `bar` parameter.
3. A context switch occurs to the server applet, and its implementation of `getShareableInterfaceObject` proceeds as described in the previous section. The server applet returns a SIO (or null).
4. `getAppletShareableInterfaceObject` returns the same SIO (or null) to its caller.

For enhanced security, the implementation shall make it impossible for the client to tell which of the following conditions caused a null value to be returned:

- The serverAID was not found.
- The server applet does not participate in inter-applet communication.
- The server applet was not communicating with this client.
- The server applet won't communicate with this client as specified by the parameter.

6.2.8 Class and Object Access Behavior

A static class field is declared when one of the following Java bytecode is executed:

`getS10, putS10, putStatic`

An object is accessed when one of the following Java bytecode is executed using the object's reference:

`getLField, putLField, invokeVirtual, invokevirtual, athrow,`

`getAField, putAField, newArray, charcast, instanceof`

`<>` refers to the various types of array bytecode, such as `ba1oad, sa1oar, etc.`

This list also includes any special or optimized forms of these bytecode that may be implemented in the Java Card VM, such as `getLField, putLField, lba1o, etc.`

Prior to performing the work of the bytecode as specified by the Java VM, the Java Card VM will perform an access check on the referenced object. If access is denied, then a `SecurityException` is thrown.

The access checks performed by the Java Card VM depend on the type and owner of the referenced object, the bytecode, and the currently active context. They are described in the following sections.

Java™ Card™ Runtime Environment (JCRE) 2.1 Specification

6.2.8.1 Accessing Static Class Fields

Dycodecs:

getStatic, putStatic

- If the JCRE is the currently active context, then access is allowed.
- Otherwise, if the bytecode is `putstatic` and the field being stored is a reference type and the reference being stored is a reference to a temporary JCRE Entry Point Object or a global array then access is denied.
- Otherwise, access is allowed.

6.2.8.2 Accessing Array Objects

Dycodecs:

<V>load, <T>store, arrayLength, checkcast, installoc

- If the JCRE is the currently active context, then access is allowed.
- Otherwise, if the bytecode is `checkcast` and the component being stored is a reference type and the reference being stored is a reference to a temporary JCRE Entry Point Object or a global array then access is denied.
- Otherwise, if the array is owned by the currently active context, then access is allowed.
- Otherwise, if the array is designated global, then access is allowed.
- Otherwise, access is denied.

6.2.8.3 Accessing Class Instance Object Fields

Dycodecs:

getfield, putfield

- If the JCRE is the currently active context, then access is allowed.
- Otherwise, if the bytecode is `getfield` and the field being stored is a reference type and the reference being stored is a reference to a temporary JCRE Entry Point Object or a global array then access is denied.
- Otherwise, if the object is owned by the currently active context, then access is allowed.
- Otherwise, access is denied.

6.2.8.4 Accessing Class Instance Object Methods

Dycodecs:

invokevirtual

- If the object is owned by the currently active context, then access is allowed. Context is switched to the object owner's context.
- Otherwise, if the object is designated a JCRE Entry Point Object, then access is allowed. Context is switched to the object owner's context.
- Otherwise, access is denied.

Java™ Card™ Runtime Environment (JCER) 2.1 Specification

6.2.8.5 Accessing Standard Interface Methods

Dycodecs:

invokesinterface

invokespecial

- If the object is owned by the currently active context, then access is allowed.
- Otherwise, if the JCRE is the currently active context, then access is allowed. Context is switched to the object owner's context.
- Otherwise, access is denied.

6.2.8.6 Accessing Shareable Interface Methods

Dycodecs:

invokespecialface

- If the object is owned by the currently active context, then access is allowed.
- Otherwise, if the object's class implements a shareable interface, and if the interface being invoked creates the shareable interface, then access is allowed. Context is switched to the object owner's context.
- Otherwise, if the JCRE is the currently active context, then access is allowed. Context is switched to the object owner's context.
- Otherwise, access is denied.

6.2.8.7 Throwing Exception Objects

By code:

- If the object is owned by the currently active context, then access is allowed.
- Otherwise, if the object is designated a JCRE Early Point Object, then access is allowed.
- Otherwise, if the JCRE is the currently active context, then access is allowed.
- Otherwise, access is denied.

6.2.8.8 Accessing Class Instance Objects

By code:

- checkcast, instanceof
 - If the object is owned by the currently active context, then access is allowed.
 - Otherwise, if the JCRE is the currently active context, then access is allowed.
 - Otherwise, if the JCRE is designated a JCRE Early Point Object, then access is allowed.
 - Otherwise, if the JCRE is the currently active context, then access is allowed.
 - Otherwise, access is denied.

6.2.8.9 Accessing Standard Interfaces

By code:

- checkcast, instanceof
 - If the object is owned by the currently active context, then access is allowed.
 - Otherwise, if the JCRE is the currently active context, then access is allowed.
 - Otherwise, access is denied.

6.2.8.10 Accessing Shareable Interfaces

By code:

- checkcast, instanceof
 - If the object is owned by the currently active context, then access is allowed.
 - Otherwise, if the object's class implements a shareable interface, and if the object is being cast into (checkcast) or is an instance of (instanceof) an interface that extends the shareable interface, then access is allowed.
 - Otherwise, if the JCRE is the currently active context, then access is allowed.
 - Otherwise, access is denied.

6.3 Transient Objects and Applet contexts

Transient objects of CLEAR_ON_RESET type behave like persistent objects in that they can be accessed only when the currently active applet context is the owner of the object (the currently active applet context at the time when the object was created).

Transient objects of CLEAR_ON_DESTROY_TYPE can only be created or accessed when the currently active applet context is the currently selected applet context. If any of the makeTransient() factory methods is called to create a CLEAR_ON_DESTROY_TYPE transient object when the currently active applet context is not the currently selected applet context, then the method shall throw a *StackUnderflowException* with reason code all.ILEGAL_TRANSIENT. If an attempt is made to access a transient object of CLEAR_ON_DESTROY_TYPE when the currently active applet context is not the currently selected applet context, the JCRE shall throw a *SecurityException*.

Applets that are part of the same package share the same group context. Every applet instance from a package shares all its object instances with all other instances from the same package. (This includes transient objects of both CLEAR_ON_RESET type and CLEAR_ON_DESTROY_TYPE owned by those applet instances.)

The transient objects of CLEAR_ON_DESTROY_TYPE owned by any applet instance within the same package shall be accessible when any of the applet instances in this package is the currently selected applet.

power is conditionally updated. The field or array component appears to be updated—reading the *oldValue* component back yields its latest conditional value—but the update is not yet committed.

When the applet calls `JCRESystem.current().transact()`, all conditional updates are committed to persistent storage. If power is lost or if some other system failure occurs prior to the completion of `JCRESystem.current().transact()`, all conditionally updated fields or array components are restored to their previous values. If the applet experiences an internal problem or decides to cancel the transaction, it can programmatically undo conditional updates by calling `JCRESystem.abortTransact()`.

7. Transactions and Atomicity

7.1 Atomicity

Atomicity defines how the card handles the contents of persistent storage after a `stop`, `failure`, or `exit` exception during an update of a single object or class field or array component. If power is lost during the update, the applet developer must be able to rely on what the field or array component contains when power is restored. The Java Card platform guarantees that any update to a single persistent object or class field will be atomic. In addition, the Java Card platform provides single-component-level atomicity for persistent arrays. That is, if the smart card loses power during the update of a data element (field) in an object/class or component of an array that shall be preserved across CAPI sessions, that data element will be restored to its previous value.

Some methods also guarantee atomicity for block updates of multiple data elements. For example, the `atomicity` of the `util.arraycopy` method guarantees that either all bytes are correctly copied or else the destination array is restored to its previous byte values.

An applet might not require atomicity for array updates. The `util.arraycopy_atomic` method is provided for this purpose. It does not use the transaction commit buffer even when called with a transaction in progress.

7.2 Transactions

An applet might need to atomically update several different fields or array components in several different objects. Either all updates take place correctly and atomically, or else all fields/components are restored to their previous values.

The Java Card platform supports a transactional model in which an applet can `disrupt` the beginning of an atomic set of updates with a call to the `JCRESystem.beginTransaction()` method. Each object update after this

7.3 Transaction Duration

A transaction always ends when the JCRE returns `java.util.concurrent.FutureReturnException` from the applet's `select`, `getCard`, `getCardInfo`, `listCards`, `call`, `commitTransact`, or `with` an abortion of the transaction (either programmatically by the applet, or by default by the JCRE). For more details on transaction abortion, refer to paragraph 7.6.

Transaction duration is the life of a transaction between the call to `JCRESystem.beginTransaction`, and either:

- a call to `commitTransact` or an abortion of the transaction,

7.4 Nested Transactions

The model currently assumes that nested transactions are not possible. There can be only one transaction in progress at a time. If `select`, `getCard`, `getCardInfo` is called while a transaction is already in progress, then a `transactionToAccept` is thrown.

The `JCRESystem.beginTransaction()` method is provided to allow you to determine if a transaction is in progress.

7.5 Tear or Reset Transaction Failure

If power is lost (`tear`) or the card is reset or some other system failure occurs while a transaction is in progress, then the JCRE shall restore to their previous values all fields and array components conditionally updated since the previous call to `JCRESystem.beginTransaction()`.

This action is performed automatically by the JCRE when it reinitializes the card after recovering from the power loss, reset, or failure. The JCRE determines which of those objects (if any) were conditionally updated, and restores them.

Note — Object `power` used by instances created during the transaction that failed due to power loss or card detect can be recovered by the JCRE.

7.6 Aborting a Transaction

Transactions can be aborted either by an applet or by the JCRCB.

7.6.1 Programmatic Abortion

If an applet encounters an internal problem or decides to cancel the transaction, it can programmatically undo conditional updates by calling `JCRESystem.abortTransaction()`. If this method is called, all conditionally updated fields and array components since the previous call to `activate()`, `beginTransaction()`, or `commit()` are restored to their previous values, and the JCRCB's `transactionDepth` value is set to 0.

7.6.2 Abortion by the JCRCB

If an update returns from the `select`, `delete`, `exec`, `process`, or `insertAll` methods with a transaction in progress, the JCRCB automatically aborts the transaction. If a return from any of `select`, `delete`, `exec`, `process`, or `insertAll` methods occurs with a transaction in progress, the JCRCB acts as if an exception was thrown.

7.6.3 Cleanup Responsibilities of the JCRCB

Object instances created during the transaction that is being aborted can be deleted only if all references to these objects can be located and converted into null. The JCRCB shall ensure that references to objects created during the aborted transaction are equivalent to a null reference.

7.7 Transient Objects

Only updates to persistent objects participate in the transaction. Updates to transient objects are never undone, regardless of whether or not they were "inside a transaction."

7.8 Commit Capacity

Since platform resources are limited, the number of bytes of conditionally updated data that can be accumulated during a transaction is limited. The Java Card technology provides methods to determine how much commit capacity is available on the implementation. The commit capacity represents an upper bound on the number of conditional byte updates available. The actual number of conditional byte updates available may be lower due to management overhead.

An exception is thrown if the commit capacity is exceeded during a transaction.

8.1.1.1 Constrained transfers with no chaining

When the no chaining mode of output transfer is requested by the applet by calling the `setOutgoingChaining` method, the following protocol sequence shall be followed.

Note – when the no chaining mode is used calls to the `waitExtension` method shall throw an `APIUsageException` with reason code `ILLEGAL_USE`.

8. API Topics

Notation

l_e = CAD expected length.

l_r = Applet response length set via `setOutgoingLength` method.

$<INS>$ = the prefix of byte equal to the incoming header INS byte, which indicates that all data bytes will be transferred next.

$<-INS>$ = the prefix of byte following the complement of the incoming header INS byte, which indicates about 1 data byte being transferred next.

$<SW1,SW2>$ = the response status bytes as in ISO7816-4.

ISO 7816-4 CASE 2

$l_e == l_r$

1. The card sends l_e bytes of output data using the standard T=0 $<INS>$ or $<-INS>$ procedure byte mechanism.

2. The card sends $<SW1,SW2>$ completion status on completion of the Applet.`process` method.

- 1. The card sends $<obj1,l_r>$ completion status bytes
- 2. The CAD sends GET RESPONSE command with $l_e = l_r$.

3. The card sends l_r bytes of output data using the standard T=0 $<INS>$ or $<-INS>$ procedure byte mechanism.

- 4. The card sends $<SW1,SW2>$ completion status to completion of the Applet.`process` method.

$l_r > l_e$

1. The card sends l_e bytes of output data using the standard T=0 $<INS>$ or $<-INS>$ procedure byte mechanism.

2. The card sends $<obj1,l_r-l_e>$ completion status bytes

- 1. The CAD sends GET RESPONSE command with new $l_e <= l_r$.
- 2. The card sends $(new) l_e$ bytes of output data using the standard T=0 $<INS>$ or $<-INS>$ procedure byte mechanism.

4. The card sends $<SW1,SW2>$ completion status to completion of the Applet.`process` method.

8.1 The APDU Class

The APDU class encapsulates access to the ISO 7816-4 based I/O across the card serial line. The APDU Class is designed to be independent of the underlying I/O transport protocol.

The JCRE may support T=0 or T=1 transport protocols or both.

8.1.1 T=0 specifics for outgoing data transfers

For compatibility with legacy CAD Implementations that do not support block chained mechanisms the APDU Class allows mode selection via the `setOutgoingLockIn`ing method.

Java™ Card™ Runtime Environment (JCRE) 2.1 Specification

Java™ Card™ Runtime Environment (JCRE) 2.1 Specification

1. Repeat steps 2-4 as necessary to send the remaining output data bytes (Lr) as required.
2. The card sends <SW1,SW2> completion status on completion of the Apdulet - process method.

[ISO 7816-4 CASE 4]

In Case 4, Lc is determined after the following initial exchange:

1. The card sends <0x61,Lr> serial bytes
2. The CAD sends GET RESPONSE command with $Lc \leq Lr$.

The rest of the protocol sequence is identical to CASE 2 described above.

If the applet aborts early and sends less than Lc bytes, zeros may be sent instead to fill out the length of the transfer expected by the CAD.

8.1.1.2 Regular Output transfers

When the no chaining mode of output transfer is not requested by the applet, zeros may be sent instead to fill out the length of the transfer expected by the CAD.

Any ISO-7816-14 compliant T=0 protocol transfer sequence may be used.

Note – The waitExtention method may be invoked by the applet between successive calls to sendByLength or sendByExtention methods. The waitExtention method shall request an additional work waiting time (ISO 7816-3) using the Dn60 procedure byte.

8.1.1.3 Additional T=0 requirements

At any time, when the T=0 output transfer protocol is in use, and the APDU class is awaiting a CTR RESPONSE command from the CAD in return to a response status of <0x00, n>, then the card, if the CAD sends a different command, the command or the sendByLength methods shall throw an APDUException with reason code ISO_70_SILENT_RESPONSE.

Calls to sendByLength or sendByExtention methods from this point on shall result in an APDUException with reason code ISO_70_APDU_ERROR. If an ISOException is thrown by the applet after the ISO_70_APDU_ERROR exception has been thrown, the JCRE shall disregard the response status in the reason code. The JCRE shall return APDU processing with the newly received command and reason APDU disqualifying.

8.1.2 T=1 specifics for outgoing data transfers

8.1.2.1 Constrained transfers with no chaining

When the no chaining mode of output transfer is requested by the applet by calling the setOutgoingChaining method, the following protocol sequence shall be followed:

Notation

Lc = CAD expected length.

Lr = Applet response length set via setOutgoingLength method.

Java™ Card™ Runtime Environment (JCRC) 2.1 Specification

The transport protocol sequence shall not use block chaining. Specifically, the M-bit (more data bit) shall not be set in the PCB of the I-blocks during the transfer (ISO 7816-3). In other words, the entire outgoing data (Lr bytes) shall be transferred in one I-block.

(If the applet aborts early and sends less than Lr bytes, zeros shall be sent instead to fill out the remaining length of the block.)

Note – When the no chaining mode is used, calls to the waitExtention method shall throw an APDUException with reason code ISO_70_SILENT_RESPONSE.

8.1.2.2 Regular Output transfers

When the no chaining mode of output transfer is not requested by the applet, the setOutgoing method is used, the following protocol sequence shall be followed:

Any ISO-7816-14 compliant T=1 protocol transfer sequence may be used.

Note – The waitExtention method may be invoked by the applet between successive calls to sendByLength or sendByExtention methods. The waitExtention method shall send an S-block command with WTX (request of IN/OUT), which is equivalent to a request of 1 additional work waiting time in T=0 mode. (See ISO 7816-3).

8.2 The security and crypto packages

The getInstance method in the following classes return an implementation instance in the context of the calling applet of the requested algorithm:

javacard.security.MessageDigest
javacard.security.Signature
javacard.security.RandomData
javacard.crypto.Cipher.

An implementation of the JCRE may implement 0 or more of the algorithms listed in the API. When an algorithm that is not implemented is requested this method shall throw a CryptoException with reason code ISO_5047_ALGORITHM.

Implementations of the above classes shall extend the corresponding base class and implement all the abstract methods. All data allocation associated with the implementation instance shall be performed at the time of instance construction to ensure that any lack of required resources can be flagged early during the installation of the applet.

Similarly, the buildKey method of the javacard.security.KeyBuilder class returns an implementation instance of the requested Key type. The JCRE may implement 0 or more types of key. When a key type that is not implemented is requested, the method shall throw a CryptoException with reason code ISO_5047_ALGORITHM.

Java Card™ Realtime Environment (JCRE) 2.1 Specification

Implementations of key types shall implement the associated interface. All data allocation associated with the key implementation instance shall be performed at the time of instance construction to ensure that any lack of required resources can be flagged early during the instantiation of the applet.

8.3 JCSystem Class

In Java Card 2.1, the getVersion method shall return (likely) 0x0201.

9. Virtual Machine Topics

The topics in this chapter detail virtual machine specifics.

9.1 Resource Failures

A lack of resources condition (such as heap space) which is recoverable shall result in a `SystemException` with reason code 10, `TRANSIENT_SYSTEM_ERROR` to indicate lack of transient space.

All other (non-recoverable) virtual machine errors such as stack overflow shall result in a virtual machine error. These conditions shall cause the virtual machine to fail. When such a non-recoverable virtual machine error occurs, an implementation can optionally require the card to be muted or blocked from further use.

Obviously, a JCIE implementer could choose to implement the installer as an applet. If so, then the installer might be coded to extend the Applet class and expand to invocations of the collect, process, and collect methods.

But a JCIE implementer could also implement the installer in other ways, as long as it provides the SELECTable behavior to the outside world. In this case, the JCIE implementer has the freedom to provide some other mechanism by which APDUs are delivered to the installer code module.

10. Applet Installer

Applet installation on smart cards using Java Card technology is a complex topic. The Java Card API 2.1 is intended to give JCIE implementers as much freedom as possible in their implementations. However, more basic common specifications are required in order to allow Java Card applets to be installed without knowing the implementation details of a particular installer.

This specification defines the concept of an installer and specifies minimal installation requirements in order to achieve interoperability across a wide range of possible installer implementations.

The Applet Installer is an optional part of the JCIE 2.1 Specification. Thus is, an implementation of the JCIE does not necessarily need to include a post-resume installer. However, if implemented, the installer is required to support the behavior specified in section 9.1.

10.1.2 Installer AID

Because the installer is SELECTable, it shall have an AID. JCIE implementers are free to choose their own AID by which their installer is selected. Multiple installers may be implemented.

10.1.3 Installer APDUs

The Java Card API 2.1 does not specify any APDUs for the installer. JCIE implementers are entirely free to choose their own APDU commands to direct their installer in its work.

The model is thus the installer on the card is driven by an installation program running on the CAD. In order for installation to succeed, this CAD installation program shall be able to:

- Recognize the card.
- SELECT the installer on the card.
- Drive the installation process by sending the appropriate APDUs to the card installer. These APDUs will contain:
 - Authentication information, to ensure that the installation is authorized.
 - The applet code to be loaded into the card's memory.
 - Linkage information to link the applet code with code already on the card.
- Instance initialization parameter data to be sent to the applet's install method.

The Java Card API 2.1 does not specify the details of the CAD installation program nor the APDUs passed between it and the installer.

10.1.4 Installer Behavior

JCIE implementers shall also define other behaviors of their installer, including:

- It receives all APDUs, like any other selected applet.
- Its design specification prescribes the various kinds and formats of APDUs that it expects to receive along with the semantics of these commands under various preconditions.
- It processes and responds to all APDUs that it receives. Incorrect APDUs are responded to with an error condition of some kind.
- When another applet is selected (or when the card is reset or when power is removed from the card), the installer becomes deselected and remains unselected until the next time that it is SELECTed.

10.1.1 Installer Implementation

The installer need not be implemented as an applet on the card. The requirement is only that the installer functionally be SELECTable. The corollary to this requirement is that installer component shall not be able to be invoked while a non-installer applet is selected nor when no applet is selected.

10.1.5 Installer Privileges

Although an installer may be implemented as an applet, an installer will typically require access to features that are not available to "other" applets. For example, depending on the JCRE implementation, the installer will need to:

- Read and write directly to memory, bypassing the object system and/or standard security.
- Access objects owned by other applets or by the JCRE.
- Invoke non-native protocol methods of the JCRE.
- Be able to invoke the `install()` method of a newly installed applet.

Again, it is up to each JCRE implementor to determine the installer implementation and supply such features in their JCRE implementations as necessary to support their installer. JCRE implementors are also responsible for the security of such features, so that they are not available to normal applets.

10.2 The Newly Installed Applet

There is a single interface between the installer and the applet that is being installed. After the installer has correctly prepared the applet for execution (performed steps such as loading and linking), the installer shall invoke the `applet.install()` method. This method is defined in the `Applet` class.

The process mechanism by which an applet's `install()` method is invoked from the installer is a JCRE implementer-defined implementation detail. However, there shall be a control switch so that any context-related operations performed by the `Install()` method (such as creating new objects) are done in the context of the new applet and not in the context of the installer. The installer shall also ensure that array objects created during applet class initialization (`Client`) initialized are also correctly by the context of the new applet.

The installation of an applet is deemed complete if all steps are completed without failure or an exception being thrown, up to and including uncaught return from executing the `Applet.register()` method. At that point, the installed applet will be selectable.

The maximum size of the parameter data is 32 bytes. And for security reasons, the `param` parameter is served `as-is`.

The maximum size of the parameter data is 32 bytes. And for security reasons, the `param` parameter is served `as-is`.

10.2.1 Installation Parameters

Other than the maximum size of 32 bytes, the Java Card API 2.1 does not specify anything about the existence of the installation parameter byte array argument. This is fully defined by the applet designer and can be in any format desired. In addition, these installation parameters are intended to be opaque to the installer.

JCRE implementers should design their installers so that it is possible for an installation program residing in a `CARD` to specify an arbitrary byte array to be delivered to the installer. The installer simply forwards this byte array to the target applet's `install()` method in the `Install` parameter. A typical implementation might define a JCRE implementation-specific `APDU` command that has the semantics "call the applet's `install()` method passing the contents of the aforementioned byte array."

II. API Constants

Some of the API classes don't have validation specified due to their constraints on *inter-module* *API*'s. If constant values are not specified consistently by implementations of this *ICRE_2.1* Specification, industry-wide interoperability is impossible. This chapter provides the required values for constants that are not specified in the *Java API 2.1 Reference*.

```

public static final byte PROTOCOL_TO = 0;
public static final byte PROTOCOL_FROM = 1;
public static final short INVALID_JOB = 5;
public static final short INVALJOB = 5;

Class javax.activation.framework.ISO7018
public final static short ISL_ISLJL_JB = 1;
public static final short BUFFER_INDICES = 2;
public static final short BAD_LENGTH = 3;
public static final short NO_ERROR = 4;
public static final short NO_VTO_CARRIER_RESPONSE = 5;

Interface javax.activation.framework.KeyBuilder
public static final byte TYPE_PLAIN, PUBLIC = 7;
public static final byte TYPE_DSA, PRIVATE = 8;
public static final byte TYPE_RSA, PUBLIC = 9;
public static final byte TYPE_RSA, PRIVATE = 10;
public static final byte TYPE_ECDH, PUBLIC = 11;
public static final byte TYPE_ECDH, PRIVATE = 12;
public static final short LENGTH_DSA_JAVA = 128;
public static final short LENGTH_DSA_JAVA = 192;
public static final short LENGTH_DSA_JAVA = 256;
public static final short LENGTH_RSA_JAVA = 192;
public static final short LENGTH_RSA_JAVA = 256;
public static final short LENGTH_RSA_JAVA = 384;
public static final short LENGTH_RSA_JAVA = 512;
public static final short LENGTH_RSA_JAVA = 1024 = 1024;
public static final short LENGTH_RSA_JAVA = 2048;
public static final short LENGTH_RSA_JAVA = 4096;
public static final short LENGTH_RSA_JAVA = 8192;
public static final short LENGTH_RSA_JAVA = 16384;
public static final short LENGTH_RSA_JAVA = 32768;
public static final short LENGTH_RSA_JAVA = 65536;
public static final short LENGTH_RSA_JAVA = 131072;
public static final short LENGTH_RSA_JAVA = 262144;
public static final short LENGTH_RSA_JAVA = 524288;
public static final short LENGTH_RSA_JAVA = 1048576;
public static final short LENGTH_RSA_JAVA = 2097152;
public static final short LENGTH_RSA_JAVA = 4194304;
public static final short LENGTH_RSA_JAVA = 8388608;
public static final short LENGTH_RSA_JAVA = 16777216;
public static final short LENGTH_RSA_JAVA = 33554432;
public static final short LENGTH_RSA_JAVA = 67108864;
public static final short LENGTH_RSA_JAVA = 134217728;
public static final short LENGTH_RSA_JAVA = 268435456;
public static final short LENGTH_RSA_JAVA = 536870912;
public static final short LENGTH_RSA_JAVA = 1073741824;
public static final short LENGTH_RSA_JAVA = 2147483648;
public static final short LENGTH_RSA_JAVA = 4294967296;
public static final short LENGTH_RSA_JAVA = 8589934592;
public static final short LENGTH_RSA_JAVA = 17179869184;
public static final short LENGTH_RSA_JAVA = 34359738368;
public static final short LENGTH_RSA_JAVA = 68719476736;
public static final short LENGTH_RSA_JAVA = 137438953472;
public static final short LENGTH_RSA_JAVA = 274877906944;
public static final short LENGTH_RSA_JAVA = 549755813888;
public static final short LENGTH_RSA_JAVA = 1099511627776;
public static final short LENGTH_RSA_JAVA = 2199023255552;
public static final short LENGTH_RSA_JAVA = 4398046511104;
public static final short LENGTH_RSA_JAVA = 8796093022208;
public static final short LENGTH_RSA_JAVA = 17592186044016;
public static final short LENGTH_RSA_JAVA = 35184372088032;
public static final short LENGTH_RSA_JAVA = 70368744176064;
public static final short LENGTH_RSA_JAVA = 140737488352128;
public static final short LENGTH_RSA_JAVA = 281474976704256;
public static final short LENGTH_RSA_JAVA = 562949953408512;
public static final short LENGTH_RSA_JAVA = 1125899906816256;
public static final short LENGTH_RSA_JAVA = 2251799813632512;
public static final short LENGTH_RSA_JAVA = 4503599627265024;
public static final short LENGTH_RSA_JAVA = 9007199254520048;
public static final short LENGTH_RSA_JAVA = 18014398509040096;
public static final short LENGTH_RSA_JAVA = 36028797018080192;
public static final short LENGTH_RSA_JAVA = 72057594036160384;
public static final short LENGTH_RSA_JAVA = 144115188072320768;
public static final short LENGTH_RSA_JAVA = 288230376144641536;
public static final short LENGTH_RSA_JAVA = 576460752289283072;
public static final short LENGTH_RSA_JAVA = 1152921504578566144;
public static final short LENGTH_RSA_JAVA = 2305843009157132288;
public static final short LENGTH_RSA_JAVA = 4611686018314264576;
public static final short LENGTH_RSA_JAVA = 9223372036628529152;
public static final short LENGTH_RSA_JAVA = 18446744073257058296;
public static final short LENGTH_RSA_JAVA = 36893488146514116592;
public static final short LENGTH_RSA_JAVA = 73786976293028232184;
public static final short LENGTH_RSA_JAVA = 147573952586056464368;
public static final short LENGTH_RSA_JAVA = 295147905172112928736;
public static final short LENGTH_RSA_JAVA = 590295810344225857472;
public static final short LENGTH_RSA_JAVA = 118059162068845171488;
public static final short LENGTH_RSA_JAVA = 236118324137688342976;
public static final short LENGTH_RSA_JAVA = 472236648275376685952;
public static final short LENGTH_RSA_JAVA = 944473296550753371904;
public static final short LENGTH_RSA_JAVA = 1888946593101506743808;
public static final short LENGTH_RSA_JAVA = 3777893186203013487616;
public static final short LENGTH_RSA_JAVA = 7555786372406026955232;
public static final short LENGTH_RSA_JAVA = 15111572744812053905464;
public static final short LENGTH_RSA_JAVA = 30223145489624107810928;
public static final short LENGTH_RSA_JAVA = 60446290979248215621856;
public static final short LENGTH_RSA_JAVA = 120892581958496431243712;
public static final short LENGTH_RSA_JAVA = 241785163916992862487424;
public static final short LENGTH_RSA_JAVA = 483570327833985724974848;
public static final short LENGTH_RSA_JAVA = 967140655667971449949696;
public static final short LENGTH_RSA_JAVA = 1934281311335942899899392;
public static final short LENGTH_RSA_JAVA = 3868562622671885799798784;
public static final short LENGTH_RSA_JAVA = 7737125245343771599597568;
public static final short LENGTH_RSA_JAVA = 15474250490687543199195136;
public static final short LENGTH_RSA_JAVA = 30948500981375086398390272;
public static final short LENGTH_RSA_JAVA = 61897001962750172796780544;
public static final short LENGTH_RSA_JAVA = 12379400392550034559356088;
public static final short LENGTH_RSA_JAVA = 24758800785100069118712176;
public static final short LENGTH_RSA_JAVA = 49517601570200138237424352;
public static final short LENGTH_RSA_JAVA = 99035203140400276474848704;
public static final short LENGTH_RSA_JAVA = 198070406280805552949697448;
public static final short LENGTH_RSA_JAVA = 396140812561611105899394896;
public static final short LENGTH_RSA_JAVA = 792281625123222211798789792;
public static final short LENGTH_RSA_JAVA = 1584563252466444423597785584;
public static final short LENGTH_RSA_JAVA = 3169126504932888847195571168;
public static final short LENGTH_RSA_JAVA = 6338253009865777694391142336;
public static final short LENGTH_RSA_JAVA = 12676506019731555388782284672;
public static final short LENGTH_RSA_JAVA = 25353012039463110777564569344;
public static final short LENGTH_RSA_JAVA = 50706024078926221555129138688;
public static final short LENGTH_RSA_JAVA = 101412048157852443110258277376;
public static final short LENGTH_RSA_JAVA = 202824096315704886220516554752;
public static final short LENGTH_RSA_JAVA = 405648192631409772441032909504;
public static final short LENGTH_RSA_JAVA = 811296385262819544882065819008;
public static final short LENGTH_RSA_JAVA = 162259277052563908976413163816;
public static final short LENGTH_RSA_JAVA = 324518554105127817952826327632;
public static final short LENGTH_RSA_JAVA = 649037108210255635905652655264;
public static final short LENGTH_RSA_JAVA = 129807421642051127871130530536;
public static final short LENGTH_RSA_JAVA = 259614843284102255742261061072;
public static final short LENGTH_RSA_JAVA = 519229686568204511484522122144;
public static final short LENGTH_RSA_JAVA = 1038459373136409022969044244288;
public static final short LENGTH_RSA_JAVA = 2076918746272818045938088488576;
public static final short LENGTH_RSA_JAVA = 4153837492545636091876176977152;
public static final short LENGTH_RSA_JAVA = 8307674985091272183752353954304;
public static final short LENGTH_RSA_JAVA = 16615349970182544367504707908608;
public static final short LENGTH_RSA_JAVA = 33230699940365088735009415817216;
public static final short LENGTH_RSA_JAVA = 66461399880730177470018831634432;
public static final short LENGTH_RSA_JAVA = 13292279976146035494003766326864;
public static final short LENGTH_RSA_JAVA = 26584559952292070988007532653728;
public static final short LENGTH_RSA_JAVA = 53169119904584141976001566317456;
public static final short LENGTH_RSA_JAVA = 10633823980916828395200313234912;
public static final short LENGTH_RSA_JAVA = 21267647961833656790400626468824;
public static final short LENGTH_RSA_JAVA = 42535295923667313580801253297648;
public static final short LENGTH_RSA_JAVA = 85070591847334627161602506595296;
public static final short LENGTH_RSA_JAVA = 170141183694669254323205013190592;
public static final short LENGTH_RSA_JAVA = 340282367389338508646410026381184;
public static final short LENGTH_RSA_JAVA = 680564734778677017292820052762368;
public static final short LENGTH_RSA_JAVA = 1361129469557354034585640105524736;
public static final short LENGTH_RSA_JAVA = 2722258939114708069171280211049472;
public static final short LENGTH_RSA_JAVA = 5444517878229416138342560422098944;
public static final short LENGTH_RSA_JAVA = 1088903575645883227668512084197888;
public static final short LENGTH_RSA_JAVA = 2177807151291766455337024168395776;
public static final short LENGTH_RSA_JAVA = 4355614302583532910674048336791552;
public static final short LENGTH_RSA_JAVA = 871122860516706582134809667358304;
public static final short LENGTH_RSA_JAVA = 1742245721033413164268193334716608;
public static final short LENGTH_RSA_JAVA = 3484491442066826328536386669433216;
public static final short LENGTH_RSA_JAVA = 6968982884133652657072773338866432;
public static final short LENGTH_RSA_JAVA = 13937965768267305314145546677732864;
public static final short LENGTH_RSA_JAVA = 27875931536534610628291093355465728;
public static final short LENGTH_RSA_JAVA = 55751863073069221256582186710931456;
public static final short LENGTH_RSA_JAVA = 11150372614613844251316437342186912;
public static final short LENGTH_RSA_JAVA = 22300745229227688502632874684373824;
public static final short LENGTH_RSA_JAVA = 44601490458455377005265749368747648;
public static final short LENGTH_RSA_JAVA = 89202980916910754010531498737495296;
public static final short LENGTH_RSA_JAVA = 178405961833821508020629977474905792;
public static final short LENGTH_RSA_JAVA = 356811923667643016041259954949811584;
public static final short LENGTH_RSA_JAVA = 713623847335286032082519919899623168;
public static final short LENGTH_RSA_JAVA = 1427247694670572064165399397798463336;
public static final short LENGTH_RSA_JAVA = 2854495389341144128330798795596926672;
public static final short LENGTH_RSA_JAVA = 5708985778682288256661597591193853344;
public static final short LENGTH_RSA_JAVA = 11417971557364575013323195182387706888;
public static final short LENGTH_RSA_JAVA = 22835943114729150026646390364775413776;
public static final short LENGTH_RSA_JAVA = 45671886229458300053292780729550827552;
public static final short LENGTH_RSA_JAVA = 91343772458916600106585561459101655056;
public static final short LENGTH_RSA_JAVA = 18268754491783320021317122918203210112;
public static final short LENGTH_RSA_JAVA = 36537508983566640042634245836406420224;
public static final short LENGTH_RSA_JAVA = 73075017967133280085268491672812840448;
public static final short LENGTH_RSA_JAVA = 146150035934266560170536983345625680896;
public static final short LENGTH_RSA_JAVA = 292300071868533120341073966691251361792;
public static final short LENGTH_RSA_JAVA = 584600143737066240682147933382502723584;
public static final short LENGTH_RSA_JAVA = 116920028544133448136429586676505545168;
public static final short LENGTH_RSA_JAVA = 233840057088266896272859173353011090336;
public static final short LENGTH_RSA_JAVA = 467680114176533792545718346706022080672;
public static final short LENGTH_RSA_JAVA = 93536022835306758509143669341204401744;
public static final short LENGTH_RSA_JAVA = 187072045670613517018287338682408803488;
public static final short LENGTH_RSA_JAVA = 374144091341227034036574677364817606976;
public static final short LENGTH_RSA_JAVA = 748288182682454068073149354729635213952;
public static final short LENGTH_RSA_JAVA = 149657636536490813614629870945927042784;
public static final short LENGTH_RSA_JAVA = 299315273072981627229259741891854085568;
public static final short LENGTH_RSA_JAVA = 59863054614596325445851948378370817136;
public static final short LENGTH_RSA_JAVA = 119726109229192650891703896756741634272;
public static final short LENGTH_RSA_JAVA = 239452218458385301783407793513483265544;
public static final short LENGTH_RSA_JAVA = 478904436916770603566815587026966531088;
public static final short LENGTH_RSA_JAVA = 957808873833541207133631174053933062176;
public static final short LENGTH_RSA_JAVA = 1915617747667082414267262348107866124352;
public static final short LENGTH_RSA_JAVA = 3831235495334164828534524696215732248704;
public static final short LENGTH_RSA_JAVA = 766247099066832965706904939243146449748;
public static final short LENGTH_RSA_JAVA = 1532494198133665811413809878486292894976;
public static final short LENGTH_RSA_JAVA = 3064988396267331622827619756972585789552;
public static final short LENGTH_RSA_JAVA = 612997679253466324565523951394517157104;
public static final short LENGTH_RSA_JAVA = 1225995358506932649131047902788234314208;
public static final short LENGTH_RSA_JAVA = 2451990717013865298262095805576468628416;
public static final short LENGTH_RSA_JAVA = 4903981434027730596524191611152937256832;
public static final short LENGTH_RSA_JAVA = 9807962868055461193048383222305874513664;
public static final short LENGTH_RSA_JAVA = 19615925736110922386096766444611749027328;
public static final short LENGTH_RSA_JAVA = 39231851472221844772193532889223498054656;
public static final short LENGTH_RSA_JAVA = 78463702944443689544387065778446996109312;
public static final short LENGTH_RSA_JAVA = 15692740588888737908877413155689399221864;
public static final short LENGTH_RSA_JAVA = 31385481177777475817754826311378798443728;
public static final short LENGTH_RSA_JAVA = 6277096235555495163550965262275759688756;
public static final short LENGTH_RSA_JAVA = 1255419247111099032710193052455151937512;
public static final short LENGTH_RSA_JAVA = 251083849422219806542038610491030387524;
public static final short LENGTH_RSA_JAVA = 502167698844439613084077220982060770488;
public static final short LENGTH_RSA_JAVA = 1004335397688879226168154441964121540976;
public static final short LENGTH_RSA_JAVA = 2008670795377758452336308883928243081952;
public static final short LENGTH_RSA_JAVA = 401734159075551690467261776785648616384;
public static final short LENGTH_RSA_JAVA = 803468318151103380934523553571297232768;
public static final short LENGTH_RSA_JAVA = 160693663630220676186906710714354465536;
public static final short LENGTH_RSA_JAVA = 321387327260441352373813421428708891072;
public static final short LENGTH_RSA_JAVA = 642774654520882704747626842857417782144;
public static final short LENGTH_RSA_JAVA = 1285549309041765409495253685744235564288;
public static final short LENGTH_RSA_JAVA = 2571098618083530818985507371488471128576;
public static final short LENGTH_RSA_JAVA = 5142197236167061637971014742976942257552;
public static final short LENGTH_RSA_JAVA = 1028439447233412327594202948595388451504;
public static final short LENGTH_RSA_JAVA = 2056878894466824655188405897190776903008;
public static final short LENGTH_RSA_JAVA = 4113757788933649310376811794381553806016;
public static final short LENGTH_RSA_JAVA = 8227515577867298620753623588763107612032;
public static final short LENGTH_RSA_JAVA = 1645503115574459724150724717752621524064;
public static final short LENGTH_RSA_JAVA = 3291006231148919448301449435505243048128;
public static final short LENGTH_RSA_JAVA = 6582012462297838896602898871010486096256;
public static final short LENGTH_RSA_JAVA = 13164024924557677793205877742020972192532;
public static final short LENGTH_RSA_JAVA = 26328049849115355586411755484041944385064;
public static final short LENGTH_RSA_JAVA = 52656099698230711172823511968083888770128;
public static final short LENGTH_RSA_JAVA = 10531219939646142234564702393616777540256;
public static final short LENGTH_RSA_JAVA = 21062439879292284469129404787233555080512;
public static final short LENGTH_RSA_JAVA = 42124879758584568938258809574467110161024;
public static final short LENGTH_RSA_JAVA = 84249759517169137876517619148934220322048;
public static final short LENGTH_RSA_JAVA = 16849951903433827575303523829786844064096;
public static final short LENGTH_RSA_JAVA = 33699903806867655150607047659573688128192;
public static final short LENGTH_RSA_JAVA = 67399807613735310301214095319147376256384;
public static final short LENGTH_RSA_JAVA = 134799615227470620602428190638294752512768;
public static final short LENGTH_RSA_JAVA = 269599230454941241204856381276589505025536;
public static final short LENGTH_RSA_JAVA = 538198460909882482409712762553179010051072;
public static final short LENGTH_RSA_JAVA = 10763969218197649648194455251063580201024;
public static final short LENGTH_RSA_JAVA = 21527938436395299296388911002127160402048;
public static final short LENGTH_RSA_JAVA = 43055876872790598592777822004254320804096;
public static final short LENGTH_RSA_JAVA = 86111753745581197185555644008508641608192;
public static final short LENGTH_RSA_JAVA = 172223507491162394371111288017017283216384;
public static final short LENGTH_RSA_JAVA = 344447014982324788742222576034034566432768;
public static final short LENGTH_RSA_JAVA = 68889402996464957748444415306806913286544;
public static final short LENGTH_RSA_JAVA = 13777880599292991549688830661361826563088;
public static final short LENGTH_RSA_JAVA = 27555761198585983099377661322723653126176;
public static final short LENGTH_RSA_JAVA = 55111522397171966198755322645447306252352;
public static final short LENGTH_RSA_JAVA = 11022304479434393239751064529089461250464;
public static final short LENGTH_RSA_JAVA = 22044608958868786479502129058178922500928;
public static final short LENGTH_RSA_JAVA = 44089217917737572959004258116357845001856;
public static final short LENGTH_RSA_JAVA = 8817843583547514591800851623271569003712;
public static final short LENGTH_RSA_JAVA = 1763568716709502918360173324654313807424;
public static final short LENGTH_RSA_JAVA = 3527137433419005836720346649308627614848;
public static final short LENGTH_RSA_JAVA = 7054274866838011673440693398617255229696;
public static final short LENGTH_RSA_JAVA = 1410854973367602334688138679723451059392;
public static final short LENGTH_RSA_JAVA = 2821709946735204669376277359446902118784;
public static final short LENGTH_RSA_JAVA = 5643419893470409338752554718893804237568;
public static final short LENGTH_RSA_JAVA = 11286839766940818675505109437787608475136;
public static final short LENGTH_RSA_JAVA = 2257367953388163735101021887557521690272;
public static final short LENGTH_RSA_JAVA = 4514735906776327470202043775115043380544;
public static final short LENGTH_RSA_JAVA = 9029471813552654940404087550230086760988;
public static final short LENGTH_RSA_JAVA = 1805894362710530988080817110046017321976;
public static final short LENGTH_RSA_JAVA = 3611788725421061976161634220092034643952;
public static final short LENGTH_RSA_JAVA = 722357745084212395232326844018406928784;
public static final short LENGTH_RSA_JAVA = 1444715490168424790464653680368138577568;
public static final short LENGTH_RSA_JAVA = 2889430980336849580929307360736277155136;
public static final short LENGTH_RSA_JAVA = 5778861960673699161858614721473554307272;
public static final short LENGTH_RSA_JAVA = 11557723921347398323717229442947106154544;
public static final short LENGTH_RSA_JAVA = 2311544784269479664743445888589421229088;
public static final short LENGTH_RSA_JAVA = 4623089568538959329486891777178842458176;
public static final short LENGTH_RSA_JAVA = 9246179137077918658973783554357684916352;
public static final short LENGTH_RSA_JAVA = 18492358274155837317947567108715369832704;
public static final short LENGTH_RSA_JAVA = 36984716548311674635895134217430739665408;
public static final short LENGTH_RSA_JAVA = 73969433096623349271790268434861579330816;
public static final short LENGTH_RSA_JAVA = 14793886619324669854358053686972315961632;
public static final short LENGTH_RSA_JAVA = 29587773238649339708716107373944631923264;
public static final short LENGTH_RSA_JAVA = 59175546477298679417432214747889263846528;
public static final short LENGTH_RSA_JAVA = 11835109295459735883464442945577852769256;
public static final short LENGTH_RSA_JAVA = 23670218590919471766928885891155705538512;
public static final short LENGTH_RSA_JAVA = 47340437181838943533857771782311411076024;
public static final short LENGTH_RSA_JAVA = 94680874363677887067715543564622822152048;
public static final short LENGTH_RSA_JAVA = 189361748727355774135431087129245644304096;
public static final short LENGTH_RSA_JAVA = 37872349745471154827086217425849288608192;
public static final short LENGTH_RSA_JAVA = 75744699490942309654172434851697777216384;
public static final short LENGTH_RSA_JAVA = 151489398981884619308344869703395554432768;
public static final short LENGTH_RSA_JAVA = 302978797963779238616689739406791108865344;
public static final short LENGTH_RSA_JAVA = 60595759592755847723337947881358221772668;
public static final short LENGTH_RSA_JAVA = 12119151918551169544667589576271644354536;
public static final short LENGTH_RSA_JAVA = 24238303837102339089335179152543288709072;
public static final short LENGTH_RSA_JAVA = 48476607674204678178670358305086577418144;
public static final short LENGTH_RSA_JAVA = 96953215348409356357340716610173154836288;
public static final short LENGTH_RSA_JAVA = 19390643069681871271468143322034630967256;
public static final short LENGTH_RSA_JAVA = 38781286139363742542936286644069261934512;
public static final short LENGTH_RSA_JAVA = 77562572278727485085872573288138523868024;
public static final short LENGTH_RSA_JAVA = 155125144557454970171745146576277047736048;
public static final short LENGTH_RSA_JAVA = 310250289114909940343490293152554955472096;
public static final short LENGTH_RSA_JAVA = 620500578229819880686980586305110910944192;
public static final short LENGTH_RSA_JAVA = 1241001156596397761373961172610220821888384;
public static final short LENGTH_RSA_JAVA = 2482002313192795522747922345220440443776768;
public static final short LENGTH_RSA_JAVA = 4964004626385591045495844690440880875553536;
public static final short LENGTH_RSA_JAVA = 992800925277118209099168938088177175110712;
public static final short LENGTH_RSA_JAVA = 198560185055423641819833787617635435022144;
public static final short LENGTH_RSA_JAVA = 397120370110847283639667575235267870044288;
public static final short LENGTH_RSA_JAVA = 794240740221694567279335150470535740088576;
public static final short LENGTH_RSA_JAVA = 158848148044338913455867030094107148177152;
public static final short LENGTH_RSA_JAVA = 317696296088
```

ଶ୍ରୀ କୃତ୍ତବ୍ୟାମିନ୍ ପାଠ୍ୟ ପଦ୍ଧତି

```
public final static byte OFFSET_AC = 4;
public final static byte OFFSET_DIAK = 5;
public final static byte CJA_1507016 = 0x00;
public final static byte IAS_ANONYC = (byte) 0x01;
public final static byte IAS_EXTERNAL_AUTHENTICATION = (byte) 0x12;
```

```
public static final byte NOT_A_TRANSACTION_OBJECT = 0;
public static final byte CLEAR_ON_RESET = 1;
public static final byte CLEAR_ON_PERSIST = 2;
```

```
public static final short ILLEGAL_VALUE = 1;
```

```
public static final short LIBRARY;
public static final short NO_TRANS;
public static final short ILLEGAL;
```

```
public static final short NO_RESOURCE = 5;
```

```
public static final short UNKNOWN_VALUE = 1;
public static final short WINTERIZATION_KEY = 2;
```

```
public static final short INVALID_INDEX = 4;  
public static final short INVALID_USB = 5;
```

```
Class java.awt.security.KeyBuilder
```

```
public static final byte TYPE_CLASSES = 1;
public static final byte TYPE_PACKAGE_PUBLIC = 4;
public static final byte TYPE_PACKAGE_PRIVATE = 5;
```

```
public static final byte TYPE_DSA_PRIVATE = 6;
public static final byte TYPE_DSA_PUBLIC = 7;
public static final byte TYPE_DSA_PRIVATE = 8;
```

```
public static final short LENGTH_OF_DESKEY = 16;
public static final short LENGTH_OF_DES3KEY = 192;
public static final short LENGTH_OF_BEAKEY = 512;
```

```
public static final short LENGTH_RSA_768 = 768;
public static final short LENGTH_RSA_1024 = 1024;
public static final short LENGTH_RSA_2048 = 2048;
```

```
public static final short LENGTHDSA_1024 = 1024;
```

```
Class javacard.security.MessageDigest  
public static final byte MD5_HA
```

```
public static final byte ALG_RIPENESS = 1;
```

```
public static final byte ALG_PSEUDO_RANDOM = 1;
public static final byte ALG_SECURE_RANDOM = 2;
```

```
public static final byte ALG_DES_3KEY = 11
```

VINTAGE December 1980 Sun Microsystems Inc

Java™ Card v2 Runtime Environment (JCRE) 2.1 Specification

```
public static final byte AAC_DES_MAC_1502797_M1 = 4;
public static final byte AAC_DES_MAC_1502797_M2 = 5;
public static final byte AAC_DES_MAC_1502797_M2 = 6;
public static final byte AAC_DES_MAC_MAC15 = 7;
public static final byte AAC_DES_MAC_MAC15 = 8;
public static final byte AAC_RSA_HA_JA09796 = 9;
public static final byte AAC_RSA_HA_JA09796 = 10;
public static final byte AAC_RSA_MAC_MAC15 = 11;
public static final byte AAC_RSA_MAC_MAC15 = 12;
public static final byte AAC_RSA_MAC_MAC15 = 13;
public static final byte AAC_RSA_MAC_MAC15 = 14;
public static final byte MODSIGN = 15;
public static final byte REDVERIFY = 16;

Class|javacard.crypto.Cipher
public static final byte AAC_DES_MAC_NOPAD = 1;
public static final byte AAC_DES_MAC_P80793_M1 = 2;
public static final byte AAC_DES_MAC_P80793_M2 = 3;
public static final byte AAC_DES_MAC_MAC5 = 4;
public static final byte AAC_DES_MAC_MAC5 = 5;
public static final byte AAC_DES_MAC_MAC5 = 6;
public static final byte AAC_DES_MAC_MAC5 = 7;
public static final byte AAC_DES_MAC_MAC5 = 8;
public static final byte AAC_DES_MAC_MAC5 = 9;
public static final byte AAC_DES_MAC_MAC5 = 10;
public static final byte AAC_DES_MAC_MAC5 = 11;
public static final byte AAC_DES_MAC_MAC5 = 12;
```

Java™ Card™ Runtime Environment (JCRE) 2.1 Specification

Java™ Card™ Runtime Environment (JCRE) 2.1 Specification

control is changed to correspond to the applet context that owns the object. When that method returns, the previous context is restored. Invocations of static methods have no effect on the currently active context. The current active context and sharing status of an object together determine if access to an object is permissible.

Currently selected applet. This ICRU keeps track of the currently selected Java Card applet. Upon receiving a SELECT command with data field = AID, the JCRE makes this applet the currently selected applet. The JCRE sends all APDU commands to the currently selected applet.

REPROMI is an acronym for **R**emotely **P**rogrammable **R**ead**O**nly **M**emory.

Firewall (see **Applet Firewall**).

Framework is the set of classes that implement the API. This includes core and extension packages. Responsibilities include dispatching of APDUs, applet selection, managing stacks, and launching applets.

Garbage collection is the process by which dynamically allocated memory is automatically reclaimed during the execution of a program.

Instance variables, also known as fields, represent a portion of an object's instant state. Each object has its own set of instance variables. Objects of the same class will have the same instance variables, but each object can have different values.

Implementation, in object-oriented programming, means to produce a particular object from its class template. This involves allocation of a data structure with the types specified by the template, and initialization of instance variables with either default values or those provided by the class' constructor function.

JAR is an acronym for Java Archive. JAR is a platform-independent file format that combines many files into one.

Java Card Runtime Environment (JCER) consists of the Java Card Virtual Machine, the framework, and the associated native methods.

JC21R1 is an acronym for the Java Card 2.1 Reference Implementation.

JCRE implementer refers to a person creating a vendor-specific implementation using the Java Card API. JCVM is an acronym for the Java Card Virtual Machine. The JCVM is the foundation of the CP card architecture. The JCVM executes byte code and manages stacks and objects. It enforces separation between applications (firewalls) and enables secure data sharing.

JDK is an acronym for Java Development Kit. The JDK is a Sun Microsystems, Inc. product that provides the environment required for programming in Java. The JDK is available for a variety of platforms, but most notably Sun Solaris and Microsoft Windows®.

Method is the name given to a procedure or routine, associated with one or more classes, in object-oriented languages.

Namespace is a set of names in which all names are unique.

Object-Oriented is a programming methodology based on the concept of an object, which is a data structure encapsulated with a set of routines, called methods, which operate on the data.

Objects, in object-oriented programming, are unique instances of a data structure defined according to the template provided by its class. Each object has its own values for the variables belonging to its class and can respond to the messages (methods) defined by its class.

Currently active context. The ICRU keeps track of the currently active Java Card applet context. When a virtual method is invoked on an object, and a context switch is required and permitted, the currently active context (See Applet execution context.)

Copyright © December 14, 1998 Sun Microsystems, Inc.

Java™ CAD™ Runtime Environment (JCER) 2.1 Specification

Package It is a namespace within the Java programming language and can have classes and interfaces. A package is the smallest unit within the Java programming language.

Persistent object Persistent objects and their values persist from one CAD session to the next, indefinitely. Objects are persistent by default. Persistent object values are updated atomically using transactions. The term persistent does not mean there is an object-oriented database on the card or that objects are serialized/deserialized; just that the objects are not lost when the card loses power.

Shareable interface Defines a set of shareable interface methods. These interface methods can be invoked from one application context when the object implementing them is obtained by another application context.

Shareable interface object (SIO) An object that implements the shareable interface.

Transaction Is an atomic operation in which the developer defines the extent of the operation by indicating in the program code the beginning and end of the transaction.

Transient object The values of transient objects do not persist from one CAD session to the next, and are stored in a certain state at specified intervals. Updates to the values of transient objects are not atomic and are not affected by transactions.

1/5/99 12:49 PM Havnor:Stuff:JCRE D2 14DEC98:READ-ME-JCRE21-DF2.txt

Page 1

Date: 16 December 1998

Dear Java Card Licensee,

JCRE21-DF2-14DEC98.zip contains a second draft of the Java Card 2.1 Runtime Environment specification, dated December 14, 1998, for Licensee review and comment. We have worked to incorporate and clarify the document based upon the review feedback we've received to date.

Complete contents of the zip archive are as follows:

- READ-ME-JCRE21-DF2.txt - This READ ME text file
- JCRE21-DF2.pdf - "Java Card Runtime Environment (JCRE) 2.1 Specification" in PDF format
- JCRE21-DF2-changebar.pdf - The revised document with change bars from the previous version for ease of review.

Summary of changes:

1. This is now a draft 2 release and will be published on the public web site shortly.
2. New description of temporary JCRE Entry Point Objects has been introduced for purposes of restricting unauthorized access. Firewall chapter 6.2.1.
3. Global arrays now have added security related restrictions similar to temporary JCRE Entry Point objects. Firewall chapter 6.2.2.
4. Detailed descriptions of the bytecodes with respect to storing restrictions for temporary JCRE Entry Point Objects and Global arrays added. Chapter 6.2.8.
5. General statement about JCRE owned exception objects added in chapter 8.
6. Corrected description of Virtual machine resource failures in transient factory methods. Chapter 9.1.

The "Java Card Runtime Environment 2.1 Specification" specifies the minimum behavior and runtime environment for a complete Java Card 2.1 implementation, as referred to by the Java Card API 2.1 and Java Card 2.1 Virtual Machine Specification documents. This specification is required to ensure compatible operation of Java Card applets. The purpose of this specification document is to bring all the JCRE elements together in a concise manner as part of the Java Card 2.1 specification suite.

Please send review comments to <javaoem-javacard@sun.com> or to my address as below. On behalf of the Java Card team, I look forward to hearing from you.

Best,
Godfrey DiGiorgi

Godfrey DiGiorgi - godfrey.digiorgi@eng.sun.com
OEM Licensee Engineering
Sun Microsystems / Java Software
+1 408 343-1506 - FAX +1 408 517-5460